UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/628,108	07/27/2000	Tatsuya Fujiyama	TSM-13	2655

24956 7590 02/08/2005

MATTINGLY, STANGER & MALUR, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/628,108	FUJIYAMA ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *May 27, 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 5-16* is/are rejected.

7)☒ Claim(s) *2-4* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed May 27, 2004 have been fully considered but they are not persuasive.

It is discussed by the applicant that the applicant's invention is directed towards allowing a user to evaluate the overall state of the system at a higher level and determine whether or not countermeasures should be applied to each of component of the system. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., evaluate the overall state of the system at a higher level) is not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

On page 20, lines 7-15 and page 21, line 12 through page 22, line 2 of the applicant's response, examples are recited and will not be addressed since they are mere allegations that which are not claimed.

The applicant argues that the teachings of Internet Scanner User Guide (ISS) "merely discloses whether to fix or patch the scanned vulnerability as opposed to allowing the user for select whether security countermeasures should be applied to a selected component." The examiner respectfully disagrees. On page 71 or ISS, it is recited that "the reports generated under the Technician category provide the most

detailed information on your network's status, including instructions for how to fix or patch the vulnerabilities detected by Internet Scanner." Furthermore, it is recited on page 81 "you can look up specific vulnerabilities and get instructions for how to fix them. Web links are provided, where possible, to make it easy for you to go directly from the online help to the correct page or Web page for the vulnerability." ISS discloses of providing information for the user to select for fixing the vulnerability. It is up to the user to select this information, otherwise, the vulnerability detected in the device (component) will not be corrected. Furthermore, by the user selecting the appropriate Web links, they are directly connected to correct patch (countermeasure) that is used to correct the detected vulnerability. The examiner fails to see a difference between the applicant's arguments and claimed invention in regards to the teachings of ISS wherein ISS fully discloses "allowing the user for select whether security countermeasures should be applied to a selected component".

The applicant argues that ISS only discloses of "information about vulnerabilities" and "provides detailed information about each vulnerability, including the vulnerability host, description, and correction actions" which is completely different from the applicant's invention. As recited in the preceding paragraph, ISS discloses on page 71 or ISS, it is recited that "the reports generated under the Technician category provide the most detailed information on your network's status, including instructions for how to fix or patch the vulnerabilities detected by Internet Scanner." Furthermore, it is recited on page 81 "you can look up specific vulnerabilities and get instructions for how to fix them. Web links are provided, where possible, to make it easy for you to go directly

from the online help to the correct page or Web page for the vulnerability." The user is given the responsibility of selected the appropriate fix or patch (countermeasure) in order to correct the detected vulnerability.

Lastly, the applicant remarks "ISS tests are only performed on actual devices to determine their vulnerability" in which the examiner fully agrees. It is further commented that ISS is "not applied to systems that are not yet existing and need to be evaluated for countermeasures" In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., applied to systems that are not yet existing) are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

2. The examiner is withdrawing the objection to the abstract since the abstract has been amended.

3. The rejection under 35 U.S.C. 112 second paragraph is hereby withdrawn by the examiner.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1 and 5-16 are rejected under 35 U.S.C. 102(b) as being anticipated by the Internet Scanner User Guide (herein referred to as ISS). The examiner notes that the applicant's claim language is in bracketed form next to the equivalent recitations of the prior art teachings.

As per claim 1, ISS discloses of a CD-ROM that contains the Internet Scanner (program comprising a method) that is installed on a (electronic) computer (pg 15). Internet Scanner is executed by the computer to evaluate the security applied to a network (system) by performing scan sessions (performing the step) on the devices (components)(pg 31). The user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network/system)(pg 31,38, and 47). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network (system)) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (system/specified first specification) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) that were

specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71). The scan results listing the detected vulnerabilities (state of security of the system) is displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) of the network (first specification system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting whether the vulnerabilities are to be executed by fixing or patching (collectively referred to as countermeasures as read from the database) the detected vulnerabilities (via a fourth step)(pg 69, 71).

As per claims 5 and 12, it is taught by ISS of database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). It is recited of reports being grouped into 4 categories (third specification) whereby executive reports handle top-level security issues (pg 69). The policy list comprises the scan types that are to be performed on the network (first specification) by scanning (evaluating) for vulnerabilities (pg 35). It is taught of the different scan tests (evaluations) that are performed to detect vulnerabilities (pg 58-59). Fixes and patches (collectively referred to as countermeasures that are preformed) are described that recommend actions taken (executed) to fix the vulnerabilities (pg 69-71, and 81). It is

interpreted by the examiner that the fixes and patches (collectively referred to as countermeasures) correspond to the executive reports as recited on page 69 and will not exceed the security level listed based on the type of report. The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network/system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input device) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71).

As per claims 6 and 13, it is taught by ISS that the user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network/system)(pg 31,38, and 47). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (first specification) by scanning (evaluating) for vulnerabilities (pg 35). It is taught of the different scan tests (evaluations) that are performed to detect vulnerabilities (pg 58-59). Fixes and patches (collectively referred to as countermeasures that are preformed) are described that recommend actions taken (executed) to fix the vulnerabilities (pg 69-71, and 81). The

scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network/system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input device) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71)

As per claims 7 and 8, ISS teaches of a CD-ROM (storage medium) that contains (stores) the Internet Scanner (program) that is installed on a (electronic) computer (pg 15). Internet Scanner is executed by the computer to evaluate the security of a network (system) by performing scan sessions (performing the step) on the devices (components)(pg 31). The user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network (system))(pg 31,38, and 47). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network (system)) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (system/specified first specification) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed (by a display unit connected to an electronic

computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71). The scan results listing the detected vulnerabilities (state of security of the system) is displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) of the network (first specification system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting whether the vulnerabilities are to be executed by fixing or patching (collectively referred to as countermeasures as read from the database) the detected vulnerabilities (via a fourth step)(pg 69, 71).

As per claim 9, ISS discloses of a CD-ROM that contains the Internet Scanner (security evaluation) that is installed on a computer (apparatus)(pg 15). The database records are retrieved listing the scan results performed (security applied to a system) during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The user (operator) selects via a graphical user interface (input unit connected to the computer) the network (first specification accepting

unit) to be scanned (evaluated) and the devices (second specification accepting unit of each of the components constituting the network/system)(pg 31,38, and 47). The policy list comprises the scan types that are to be performed on the network (specified first specification accepting unit) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed in a window based upon the scanning (evaluating) of the devices (second specification accepting unit of each of the components constituting the network /system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented the option of selecting (via the third specification accepting unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71). The scan results listing the detected vulnerabilities (state of security of the system) is displayed in a window based upon the scanning (evaluating unit) of the devices (second specification accepting unit of each of the components constituting the network/system) of the network (first specification accepting unit) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented the option of selecting whether the vulnerabilities are to be executed by fixing or patching (collectively referred to as countermeasures as read from the database) the detected vulnerabilities (state of security)(pg 69, 71).

As per claim 10, ISS discloses of a CD-ROM that contains the Internet Scanner (program comprising a method) that is installed on a (electronic) computer (pg 15). The Internet Scanner provides information (support formation) about patches and fixes (collectively referred to as countermeasures) to a user (pg 69-71). Internet Scanner is executed by the computer to evaluate the security of a network (system) by performing

scan sessions (performing the step) on the devices (components)(pg 31). The user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network/system)(pg 31,38, and 47). Fixes and patches (collectively referred to as countermeasures) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (system/specified first specification) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network/system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71).

As per claim 11, it is taught by ISS of database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (first

specification) by scanning (evaluating) for vulnerabilities (pg 35). It is taught of the different scan tests (evaluations) that are performed to detect vulnerabilities (pg 58-59). Fixes and patches (collectively referred to as countermeasures) are described (support formation) that recommend actions taken (executed) to fix the vulnerabilities (pg 69-71, and 81). It is interpreted by the examiner that the fixes and patches (collectively referred to as countermeasures) correspond to the respective items listed on page 58-59 that are evaluated during the scan tests during the reading out from the database during a second step. The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network/system) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the display) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71).

As per claims 14 and 15, ISS teaches of a CD-ROM (storage medium) that contains (stores) the Internet Scanner (program) that is installed on a (electronic) computer (pg 15). Internet Scanner is executed by the computer to evaluate the security of a network (system) by performing scan sessions (performing the step) on the devices (components)(pg 31). The user (operator) selects (by a first step) via a graphical user interface (input unit connected to the computer) the network (first specification of a system) to be scanned (evaluated) and the devices (second specification of each of the components constituting the network (system))(pg 31,38,

and 47). Fixes and patches (collectively referred to as countermeasures that are preformed) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification of each of the constituent components of the network/system) (pg 31,70, and 98). The policy list comprises the scan types that are to be performed on the network (system/specified first specification) by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed (by a display unit connected to an electronic computer) in a window based upon the scanning (evaluating) of the devices (second specification of each of the components constituting the network (system)) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented (via a third step) the option of selecting (via the input unit) whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71).

As per claim 16, ISS discloses of a CD-ROM that contains the Internet Scanner (security construction support apparatus) that is installed on a computer (pg 15). The database records are retrieved listing the scan results performed during the scan sessions on the devices (second specification accepting unit of each of the constituent components of the network) (pg 31,70, and 98). Fixes and patches (collectively referred to as countermeasures that are preformed) are described that recommend actions taken to fix the vulnerabilities (pg 69-71, and 81). The user (operator) selects via a graphical user interface (input unit connected to the computer) the network (first specification accepting unit) to be scanned (evaluated) and the devices (second

specification accepting unit of each of the components constituting the network/system)(pg 31,38, and 47). The policy list comprises the scan types that are to be performed on the network by scanning (evaluating) for vulnerabilities (pg 35). The scan results are displayed in a window based upon the scanning (evaluating) of the devices (second specification accepting unit of each of the components constituting the network) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented the option of selecting whether the vulnerabilities are to be fixed or patched (collectively referred to as countermeasures as read from the database)(pg 69, 71). The scan results listing the detected vulnerabilities (state of security of the system) is displayed (via a security countermeasure display unit) in a window based upon the scanning of the devices (second specification accepting unit of each of the components constituting the network/system) of the network (first specification accepting unit) that were specified by the user (operator)(pg 31,38, and 49). The user (operator) is presented the option of selecting whether the vulnerabilities are to be executed by fixing or patching (collectively referred to as countermeasures as read from memory) the detected vulnerabilities (state of security)(pg 69, 71).

Allowable Subject Matter

1. Claims 2-4 would be allowable if rewritten to overcome the rejection under 35 U.S.C. 112, second paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

As per claim 2, it was not found to be taught in the prior art of for each security type, determining the ratio of the number of security countermeasures accepted as executed to the number of security countermeasures classified into the security type concerned and displaying a degree of accomplishment of the security countermeasures classified into the security type.

As per claim 3, it was not found to be taught in the prior art of determining the total sum of degrees of risks corresponding to the security countermeasures accepted as non-executed out of the security countermeasures classified into a security type and displaying the total sum of the degrees of risk for each of the security types as a degree of the remaining risk of the security countermeasures classified into the respective security types.

As per claim 4, it was not found to be taught in the prior art of determining the total sum of the costs corresponding to the security countermeasures accepted as executed out of the security countermeasures classified into a security type and displaying the total sum of the costs for each of the security types as the required cost of the security countermeasures classified into the security type.

Conclusion

2. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

2/2/05

CR

February 2, 2005